UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
v.	:	**13-cr-761 (VM)**
YUDONG ZHU **YE LI,**	:	**Electronically Filed**
Defendants.	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT YUDONG ZHU'S MOTION TO SUPPRESS EVIDENCE SEIZED FROM LAPTOP COMPUTER AND THE FRUITS OF SUCH EVIDENCE

John D. Cline
Law Office of John D. Cline
235 Montgomery Street, Suite 1070
San Francisco, CA 94104
(415) 322-8319 (telephone)

Maurice H. Sercarz
Sercarz & Riopelle, LLP
810 Seventh Avenue, Suite 620
New York, NY 10019
(212) 586-4900 (telephone)

Attorneys for Dr. Yudong Zhu

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

OTHER AUTHORITIES

Dr. Yudong Zhu submits this memorandum in support of his motion to suppress the contents of the laptop computer that he surrendered to NYU in May 2013. As we demonstrate below, (1) Dr. Zhu had a legitimate expectation of privacy in the contents of the computer, which he had protected with multiple passwords and encrypted; (2) NYU--which did not know the passwords or how to undo the encryption--lacked actual or apparent authority to consent to the search of the computer; and (3) the government's warrantless search of the computer therefore violated Dr. Zhu's rights under the Fourth Amendment. The evidence obtained from the computer, and the fruits of that evidence, must be suppressed.

We have found no case upholding third-party consent to search a password-protected, encrypted computer where the searching officer knows that the person giving the consent does not have the password and does not know how to undo the encryption. The government thus seeks a novel expansion of one of the "few jealously and carefully drawn exceptions" to the warrant requirement. *United States v. Buettner-Janusch*, 646 F.2d 759, 764 (2d Cir. 1981) (quotation omitted). The Court should decline the government's invitation.

STATEMENT OF FACTS

Dr. Zhu began work as an Assistant Professor in the Department of Radiology at the NYU School of Medicine on October 27, 2008. He was promoted to Associate Professor in September 2012. His expertise was (and is) in magnetic resonance imaging (MRI). Declaration of Dr. Yudong Zhu ("Zhu Dec.") ¶ 2.

In 2010, Dr. Zhu, through NYU, applied for a substantial grant from the National Institutes of Health (NIH) to conduct MRI research. NIH awarded the grant in May 2011. Dr. Zhu was the principal investigator on the grant. Zhu Dec. ¶ 3.

In August 2011, Dr. Zhu directed that a portion of the grant funds be spent to purchase a laptop computer for his use. Dr. Zhu ordered the laptop through NYU. It was delivered directly to Dr. Zhu's NYU office in September 2011. Dr. Zhu configured the laptop himself; no one from NYU was involved. He established several levels of passwords. He also implemented encryption, which required a password before the hard disk could be accessed. Dr. Zhu did not provide those passwords to anyone else, within or outside of NYU. He did not give anyone, within or outside of NYU, access to the laptop's contents. Although Dr. Zhu had an office to himself at NYU for which he controlled the key, he did not leave the laptop in the office overnight. Zhu Dec. ¶ 4.

Dr. Zhu used the laptop for work on the NIH grant and NYU matters, and for the full range of professional and personal purposes. It was the only portable computer that he used between September 2011 and May 2013. In addition to sensitive information relating to MRI-related work that he and others carried out, he kept on the laptop personal information relating to his family's and his finances, health, and other private matters. The laptop did not include any "banner" or other routine warning against personal use. Zhu Dec. ¶ 5. Dr. Zhu expected that the contents of the laptop would remain private and would not be exposed to anyone within or outside of NYU without his consent. Zhu Dec. ¶ 6.

In early 2013, NYU began investigating Dr. Zhu and two of his research assistants. On May 8, 2013, lawyers for NYU and an NYU vice-president questioned Dr. Zhu, who was unrepresented. During the questioning, the NYU lawyers asked Dr. Zhu to turn over the laptop and provide his passwords. Dr. Zhu surrendered the computer but refused requests for the passwords. Zhu Dec. ¶ 7.

On May 10, 2013, Reginald Odom, a vice-president at NYU Medical Center, sent Dr. Zhu an email with two attachments: a "Policy Statement on Privacy, Information Security, and Confidentiality" that Dr. Zhu signed on October 20, 2008, and an excerpt from the NYU Medical Center "Human Resources Policies and Procedures." The 2008 Policy provides in part:

> 13. I understand that the *confidential information* and software I use for my job are not to be used for personal benefit or to benefit another unauthorized institution. I also understand that my institution may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures.

Declaration of John D. Cline ("Cline Dec."), Ex. 1, at 4 (italics in original); Zhu Dec. ¶ 8. The "Human Resources Policies and Procedures," which notes that it was revised in "9/2010," provides in part:

> Employees do not have, nor should they reasonably expect to have, a right to privacy concerning any information contained on, or transmitted through, electronic storage media that are the property of, or provided by, the Medical Center. All employees are encouraged and advised to keep personal records at home. The Medical Center reserves the right to monitor its electronic communication systems and equipment (such as computer hard drives, network drives, electronic mail and voicemail).

Cline Dec., Ex. 1, at 2. Dr. Zhu does not recall receiving or reviewing the 2010 Policy at any point before Mr. Odom sent it to him. Zhu Dec. ¶ 8.

Following the May 8 questioning, Dr. Zhu requested return of the laptop so he could proceed with his research. Mr. Odom responded on May 13. He stated that the laptop would not be returned until NYU completed its investigation by imaging and reviewing the documents it contained. He added: "To facilitate this process being resolved expeditiously we asked you for the password(s) necessary to access your laptop and you have refused to provide them." Mr. Odom warned Dr. Zhu that if he failed to provide the passwords within one business day, NYU would "treat your actions as insubordination and . . . initiate actions necessary to terminate your employment and faculty appointment." Cline Dec., Ex. 2, at 1.

The next day, Dr. Zhu reaffirmed his position and refused to provide the passwords. He explained: "I decline to give you my password on the ground that I must safeguard the privacy of my family, proprietary information originating from my collaborators, and plans for addressing important research problems. . . . As I emphasized during the meeting, in my collaboration with Professor Chen under the framework of his research grant project, he asked me to use an email account provided by him to ensure the security of proprietary information originating from some members of the project team that are required in carrying out the project. I am not in a position to grant you access to such information." Cline Dec., Ex. 2, at 2.

On May 16, 2013, Dr. Zhu further explained his position to NYU:

> 1) I think the laptop belongs to the government not NYU. I purchased it on my own using the R01 research grant that NIH awarded to me. And I did not get NYU involved in setting up the laptop or its software.
>
> 2) Even though I have an office all to myself at the school and I control the key to the office, I never leave the laptop overnight in my office. I always use password and encryption to protect the content of the laptop.
>
> 3) I spend a lot of time working when I commute and on my own time at home. Being the only portable computer I use, I have both NYU and non-NYU content on it. But I have always expected full rights to the non-NYU content on the laptop, including my privacy right. The password and the encryption are part of the means I apply to ensure my rights.

Cline Dec., Ex. 2, at 3.

After the May 8, 2013 interview of Dr. Zhu, NYU contacted the DOJ about Dr. Zhu. The FBI and United States Attorneys' Office investigated, and on May 19, 2013 the government filed a criminal complaint against Dr. Zhu and his two research assistants.

At some point after Dr. Zhu surrendered his laptop on May 8, NYU provided it to a computer forensic firm, Stroz Friedberg. Stroz did not decrypt and image Dr. Zhu's computer. Instead, at NYU's request, it provided the still-encrypted computer to the FBI. On June 27, 2013, Annette Johnson, General Counsel of the NYU Medical Center, signed a "Consent to Search

Computer(s)" form. Cline Dec., Ex. 3. The FBI then decrypted the laptop and imaged its contents. The government never obtained a warrant to search the computer.

On October 2, 2013, the government obtained an indictment against Dr. Zhu and one of his research assistants. The indictment charges Dr. Zhu with honest services fraud, conspiracy, and other offenses. Dr. Zhu now seeks to suppress all evidence obtained from the search of the laptop computer and the fruits of such evidence.

ARGUMENT

As we demonstrate in the following parts, (1) Dr. Zhu has standing to contest the search of the laptop; (2) NYU lacked actual or apparent authority to consent to the search of the laptop and thus the government's warrantless search violated the Fourth Amendment; and (3) the evidence obtained from a search of the laptop, and the fruits of that evidence, must be suppressed.

I. DR. ZHU HAD A LEGITIMATE EXPECTATION OF PRIVACY IN THE CONTENTS OF THE LAPTOP COMPUTER.

Dr. Zhu had a legitimate expectation of privacy in the password-protected, encrypted laptop that he alone accessed and used. He therefore has standing to challenge the government's search of its contents.

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois,* 439 U.S. 128, 143 (1978)); *see, e.g., United States v. Pena*, 961 F.2d 333, 336-37 (2d Cir. 1992); *United States v. Osorio*, 949 F.2d 38, 40 (2d Cir. 1991). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." *Hamilton*,

538 F.3d at 167 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)); *see, e.g., Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (applying principles to search of public employee's office computer and finding employee had standing).

A. Dr. Zhu Had a Subjective Expectation of Privacy in the Contents of the Laptop.

The first prong of the Fourth Amendment standing analysis--the subjective expectation of privacy--is easily met in this case. In *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), the Ninth Circuit, under similar circumstances, noted that the government did not even contest a defendant's "claim that he had a subjective expectation of privacy in his office and the computer. The use of a password on his computer and the lock on his private office door are sufficient evidence of such expectation." *Id*. at 1189.

As in *Ziegler*, Dr. Zhu had a subjective expectation of privacy in the contents of the password-protected, encrypted laptop computer. Dr. Zhu protected the laptop by several levels of passwords and by encryption. He refused to disclose those passwords to his employer despite repeated requests backed by a threat of termination. Dr. Zhu did not provide the passwords to anyone else. He did not give anyone access to the contents of the laptop. Zhu Dec. ¶ 5. He expected that the contents of the laptop would remain private and would not be exposed to anyone without his consent. Zhu Dec. ¶ 6. Dr. Zhu's subjective beliefs are further evidenced by his email to NYU asserting that he "always expected the full rights to the non-NYU content on the laptop, including my privacy right. The password and encryption are part of the means I apply to ensure my rights." Cline Dec. Ex. 2, at 3. Under these circumstances, Dr. Zhu's subjective expectation of privacy cannot seriously be disputed. *See, e.g., United States v. Slanina*, 283 F.3d 670, 676 (5th Cir.) (employee "clearly demonstrated a subjective expectation

of privacy" where he installed password on office computer), *vacated on other grounds*, 537 U.S. 802 (2002).

B. Dr. Zhu's Expectation of Privacy Was Reasonable.

Dr. Zhu's expectation of privacy "is one that society accepts as reasonable." *Hamilton*, 538 F.3d at 167. He ordered the laptop computer and configured it; he protected the laptop with passwords and encryption; he alone had access to it; he did not permit anyone else to use it; he used it for personal matters, as well as for work; and he kept it in his possession and control, rather than--for example--leaving it in his NYU office. Zhu Dec. ¶¶ 4, 5.

An employee's use of a password weighs in favor of finding a reasonable expectation of privacy in the contents of a work computer. *See, e.g., Slanina*, 283 F.3d at 676-77 (employee had reasonable expectation of privacy in his computer and files where the employee had installed passwords to limit access); *United States v. Reeves*, 2012 U.S. Dist. LEXIS 68962, at *23-*24 (D.N.J. May 17, 2012) ("In addition, Meloney's computer was password protected. While her password was commonly known at the work place among her fellow employees, it was not known to the public and could not be accessed by anyone outside this small, closely held corporation. This is sufficient to show her intent to exclude members of the public and maintain privacy in the documents kept on her computer, an expectation shared with the business owner."); *United States v. Howe*, 2011 U.S. Dist. LEXIS 57491, at *18-*20 (W.D.N.Y. May 27, 2011) (reasonable expectation of privacy even where defendant gave password to computer repairmen); *United States v. Robson*, 2007 U.S. Dist. LEXIS 53627 (E.D. Mich. July 24, 2007) ("[H]is use of a password to protect his user profile shows his right to exclude others from accessing those files, even if such a password would not necessarily prevent access to the hard drive through the use of specialized forensic software."). Here, Dr. Zhu protected the contents of

the laptop computer through several levels of passwords and through encryption. He did not share those passwords with anyone at NYU, and in fact expressly refused to provide the passwords to NYU, despite repeated requests.

In addition to password-protection, other steps to restrict third-party use or access to the computer also weigh in favor of finding a reasonable expectation of privacy in its contents. *See, e.g., Leventhal,* 266 F.3d at 73-74. In *Leventhal*, the employee "had exclusive use of the desk, filing cabinet, and computer in his office [and] did not share use of his computer with other employees in the Accounting Bureau nor was there evidence that visitors or the public had access to his computer." *Id*. Dr. Zhu's expectation of privacy was even more clearly reasonable than that of the employee in *Leventhal*. Although Dr. Zhu had a private office at NYU, his practice was not to leave the laptop there overnight. He used passwords and encryption to protect the laptop's contents, and he did not share the passwords with anyone. NYU was not involved in setting up the laptop or its software. Dr. Zhu did not give anyone from NYU access to the laptop's contents. Zhu Dec. ¶¶ 4, 5.

An expectation of privacy is more likely to be found reasonable where the employer does not have either "a general practice of routinely conducting searches of office computers or [placing the employee] on notice that he should have no expectation of privacy in the contents of his office computer." *Leventhal*, 266 F.3d at 73-74. In *Leventhal*, the Second Circuit noted that although the employer's "technical support staff had access to all computers in the DOT offices, their maintenance of these computers was normally announced and the one example in the record of an unannounced visit to [the employee's] computer was only to change the name of a server." *Id.* at 74. Technical support personnel also had access to employee computers "to search for a document in an unattended computer, but there was no evidence that these searches were

frequent, widespread, or extensive enough to constitute an atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable." *Id.* (quotation omitted). The Second Circuit thus concluded that "[t]his type of infrequent and selective search for maintenance purposes or to retrieve a needed document, justified by reference to the 'special needs' of employers to pursue legitimate work-related objectives, does not destroy any underlying expectation of privacy that an employee could otherwise possess in the contents of an office computer." *Id.*

The NYU policy for monitoring or accessing Dr. Zhu's computer was even less invasive than in *Leventhal*. The NYU policy Dr. Zhu received and signed provided: "I also understand that my institution may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures." Cline Dec. Ex. 1, at 4. In practice, this policy had little significance. During the entire time Dr. Zhu possessed and used the laptop, no one from NYU requested access to it or its contents until May 2013, when the investigation began that led to the charges in this case--and even then he refused to provide the passwords. Zhu Dec. ¶ 9. To Dr. Zhu's knowledge, NYU has not requested access to the computers of other NYU professors, much less maintained "a general practice of routinely conducting searches of office computers." *Leventhal*, 266 F.3d at 74; *see* Zhu Dec. ¶ 9.

Nor did NYU maintain and disseminate a policy banning the storage of personal material on a work computer--a factor some courts have found to weigh against a reasonable expectation of privacy. The only NYU policy Dr. Zhu signed on this subject provided: "I understand that the *confidential information* and software I use for my job are not to be used for personal benefit or to benefit another unauthorized institution." Nothing in this policy banned personal use of the laptop computer. The 2010 Policy, which Dr. Zhu does not recall receiving or reviewing before

Mr. Odom sent it to him in May 2013, provided that "[a]ll employees are encouraged and advised to keep personal records at home," and it prohibited "[e]xcessive or inappropriate personal use" of NYU computers. But the 2010 Policy did not ban--and in fact by implication permitted--personal use that was not excessive or inappropriate. While the 2010 Policy includes a statement that "[e]mployees do not have, nor should they reasonably expect to have, a right to privacy," such a blanket statement does not deprive employees of any reasonable expectation of privacy--particularly when the statement is neither widely disseminated (by banners displayed each time a computer starts up, for example) nor routinely enforced. *See, e.g., Leventhal*, 266 F.3d at 74 (employee had reasonable expectation of privacy in contents of work computer where the employer policy "did not prohibit the mere storage of personal materials in his office computer"); *Slanina*, 283 F.3d at 676-77 (employee had reasonable expectation of privacy in private computer files, despite computer screen warning that there shall be no expectation of privacy in using employer's computer system, where "employees [we]re allowed to use their work computers for private communications"); *Convertino v. DOJ*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (factor supporting an employee's expectation of privacy as reasonable included that the "DOJ maintains a policy that does not ban personal use of the company e-mail").

For these reasons, Dr. Zhu's expectation of privacy in the contents of the laptop computer was reasonable. He thus has standing to contest the government's search.

II. THE GOVERNMENT CANNOT ESTABLISH THAT NYU HAD ACTUAL OR APPARENT AUTHORITY TO CONSENT TO THE SEARCH OF THE LAPTOP COMPUTER.

The government did not obtain a warrant to search the laptop computer. Instead, it relied solely on the purported consent from NYU. Because the government cannot establish that NYU had either actual or apparent authority to consent to the search of the laptop, the search violated Dr. Zhu's Fourth Amendment rights.

"It is basic Fourth Amendment jurisprudence that when the Government seeks to intrude upon an individual's legitimate expectations of privacy, it must either obtain a warrant from a neutral magistrate or bring its search within one of the few 'jealously and carefully drawn' exceptions to the warrant requirement." *Buettner-Janusch*, 646 F.2d at 764 (quoting *Jones v. United States*, 357 U.S. 493, 499 (1958)). One of those "jealously and carefully drawn exceptions to the warrant requirement" is valid third-party consent. *See, e.g., Georgia v. Randolph*, 547 U.S. 103, 109 (2006). "To satisfy the burdens imposed on it by the third party consent principle, the Government must show, by a preponderance of the evidence, that the consent to search was freely and voluntarily given and was obtained from someone who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *Buettner-Janusch*, 646 F.2d at 764 (quotation and citations omitted).

The key question here is whether the government can prove that NYU satisfied the "common authority" prong of this standard. As the Supreme Court explained:

> Common authority is, of course, not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (citations omitted).

A. The Government Cannot Establish That NYU Had Actual Authority to Consent to the Search of the Laptop.

In the Second Circuit, "a third-party consent to a search will validate the search if two prongs are present: first, the third party had access to the area searched, and, second, either: (a) common authority over the area; or (b) a substantial interest in the area; or (c) permission to gain access." *United States v. Davis*, 967 F.2d 84, 87 (2d Cir. 1992); *see, e.g., Moore v. Andreno*, 505

F.3d 203, 209-10 (2d Cir. 2007). The government cannot satisfy either of those requirements in this case. As we discuss below, that Dr. Zhu password-protected and encrypted the laptop's contents and did not share the passwords with NYU--facts known to the government agents who conducted the search--defeats any reliance on NYU's consent. *See, e.g., Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (where computer user concealed password for certain files from co-user, co-user could not consent to search of those files); *United States v. Griswold*, 2011 U.S. Dist. LEXIS 153943, at *17-*25 (W.D.N.Y. June 2, 2011) (mother who did not know password to son's computer could not consent to search); *cf. Randolph*, 547 U.S. at 135 (Roberts, C.J., dissenting) ("To the extent a person wants to ensure that his possessions will be subject to a consent search only due to his *own* consent, he is free to place these items in an area over which others do *not* share access and control, be it a private room or a locked suitcase under a bed.") (emphasis in original).

1. NYU Lacked Access to the Contents of the Laptop.

Because Dr. Zhu password-protected and encrypted the laptop, NYU did not have "access to" its contents. *Davis*, 967 F.2d at 87. While NYU may (or may not) have "had the right to retrieve the laptop from [Dr. Zhu] and deliver it to the [FBI], the laptop itself is akin to a closed container that has been 'locked' by [Dr. Zhu's] deliberate use of a password." *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *11. NYU did not have actual authority to consent to the search, because NYU did not have access to "the area searched"--the *contents* of the laptop computer.

2. NYU Lacked Common Authority Over, a Substantial Interest in, or Permission to Gain Access to the Contents of the Laptop.

The government similarly cannot satisfy the second prong of the actual authority analysis, because NYU did not have "common authority over" the contents of the laptop, a

"substantial interest in" the contents of the laptop, or "permission to gain access to" the contents of the laptop.

First, NYU did not have "common authority" over the contents of the laptop computer. No one from NYU was involved in setting up the computer; Dr. Zhu did not share the passwords with NYU; and no NYU personnel had ever accessed the laptop. Second, NYU did not have a "substantial interest" in the contents of the laptop. The laptop was purchased with funds from the NIH grant; NYU did not pay for it. The laptop was delivered directly to Dr. Zhu's office in September 2011 in its original packaging. He set it up without any involvement by NYU, set several levels of passwords and encryption, did not share those passwords with anyone at NYU, and continued to use the laptop for the next year and a half with sole access. At no time before May 2013 did NYU seek access to the contents of the laptop. Finally, Dr. Zhu expressly denied "permission to gain access to" the contents of the laptop when he refused to provide the passwords.

As noted above, the fact that NYU did not know the passwords for the laptop is particularly significant. Courts have held repeatedly that a third party who does not have the password for computer files lacks actual authority to consent to a search of those files. *See, e.g., United States v. Buckner,* 473 F.3d 551, 554 (4th Cir. 2007) (a co-user of a computer "did not have actual authority to consent to a search of her husband's password-protected files because she did not share mutual use, general access or common authority over those files").[1] In *Trulock*,

---

[1] In *Buckner*, the court of appeals concluded that the co-user (defendant's wife) had apparent authority to consent to the search of password-protected files. But the court emphasized that the searching officers did not know the files were password-protected, 473 F.3d at 555; the computer was not encrypted, *id*. at 553 n.1; and the computer was located in a common area and was leased and used by the wife, *id*. at 555. Here, by contrast (as discussed below), the FBI agents who searched the laptop knew that it was password protected and encrypted and knew that NYU

the Fourth Circuit analogized the situation to a locked footlocker inside a bedroom and explained that although the co-user of the computer "had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files." 275 F.3d at 403. Here, NYU was not even a co-user of the laptop computer, and Dr. Zhu password-protected access to the entire laptop and encrypted it as well. NYU therefore lacked actual authority to consent to a warrantless search of the password-protected or "locked" contents of the laptop computer.[2]

B. The Government Cannot Establish That NYU Had Apparent Authority to Consent to the Search of the Laptop.

Because NYU lacked actual authority to consent to a law enforcement search of the laptop, the government must depend on NYU's apparent authority. But it cannot establish that form of authority either.

The critical inquiry when the government relies on apparent authority is an objective one: "[W]ould the facts available to the officer at the time the consent is given warrant a person of reasonable caution in the belief that the consenting party had authority over the item to be searched?" *United States v. James*, 353 F.3d 606, 615 (8th Cir. 2003); *see, e.g., Illinois v.*

---

did not have the passwords. Whether the agents also knew that Dr. Zhu was the exclusive user of the computer and kept it in his exclusive possession before surrendering it to NYU in May 2013 is unclear on the current record; those facts must await further evidentiary development.

[2] Even if NYU had actual authority to search the laptop itself for its own purposes (which it did not), it lacked authority to consent to a law enforcement search. As one federal court observed, "A search may be valid for one purpose and valid when conducted by certain individuals, but invalid if done for another purpose and done by other individuals." *United States v. Sims*, 2001 U.S. Dist. LEXIS 25819, at *22 (D.N.M. 2001). In other words, "simply because someone could search [the laptop] computer does not mean that law enforcement could. . . . The fact remains that this was a law enforcement search, and as such, should have been conducted pursuant to a warrant." *Id.* at *22-*23. Thus, even if NYU's policies entitled *NYU* to gain access to the contents of Dr. Zhu's computer (they did not, for the reasons noted above), those policies did not give NYU authority to consent to a *law enforcement* search of those same materials.

Rodriguez, 497 U.S. 177, 188 (1990). In the context of third-party authority to search a laptop computer, courts frame the inquiry as whether "reasonable officers, given the information that [the law enforcement officers] possessed, [would] believe that [the third party] had joint control of the files within the laptop sufficient to authorize [the third party] to consent to the search of [the] laptop?" *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *13.

As with the actual authority inquiry, the existence of a password is often decisive in the apparent authority context. "Password protected computers or files have been likened to private, locked compartments, so that where officers know that the person offering consent lacks the key, or password, they cannot reasonably conclude that the person in question has the authority to consent to a search of any 'locked' areas." *United States v. Cole*, 2008 U.S. Dist. LEXIS 57437, at *10 (D. Me. July 24, 2008), *adopted*, 2008 U.S. Dist. LEXIS 61614 (D. Me. Aug. 12, 2008).[3] Here, the government undoubtedly knew before it searched the laptop that NYU lacked the necessary passwords.[4] It received the laptop from Stroz Friedberg--which had been retained by NYU--in encrypted form and used forensic tools to bypass the passwords and decrypt the contents. In other words, "before looking at any files on the computer, [the FBI] was aware that

---

[3] In *Cole*, the district court found that the third party (Presby) had authority to consent to search of the computer where "[i]t is undisputed that Presby selected the computer, purchased it on his credit, set up the user accounts, and was the primary administrator with respect to the computer. He was the individual responsible for 'fixing' things when there were software or security problems and he had ready access to Cole's desktop user account, notwithstanding the password protection that may have restricted access to Cole's account by someone other than Presby or Cole." 2008 U.S. Dist. LEXIS 57437, at *11. None of these circumstances exists here. NIH funds were used to purchase the laptop, not NYU funds. Dr. Zhu selected the computer, set up the computer, was the sole user and "administrator" of the computer, and was responsible for fixing problems with the computer. Because of the password protection and encryption he installed, he alone--and not NYU--had access to the computer.

[4] To the extent the government disputes this or any other material factual question, Dr. Zhu requests an evidentiary hearing. *See Robson*, 2007 U.S. Dist. LEXIS 53627, at *19 (ordering evidentiary hearing to determine if person giving third-party consent informed searching officers about password to which she did not have access).

the laptop had been 'locked' but nevertheless used a 'special forensic tool' to 'bypass a password' and gain access to the files on the hard drive." *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *17. The presence of passwords and encryption on the laptop, and NYU's inability to provide those passwords or to undo the encryption, made it impossible for a reasonable officer to believe that NYU had actual authority over the contents of the laptop. *See, e.g., Robson*, 2007 U.S. Dist. LEXIS 53627, at *18-*19 (if mother alerted searching officers that son's files were protected by a password to which she did not have access, "then concluding that her authority extended to those files becomes unreasonable").

"[T]he type and location of the computer" also bear on the apparent authority question. *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *14. Thus, "[a] portable laptop computer kept in a bedroom belonging to an adult suggests a greater privacy interest in the computer's files than a desktop computer located in a common area that is readily accessible to a number of different users." *Id*. Here, the searching FBI agents knew the computer was a "portable laptop"--and of course they knew it was password protected and encrypted. Whether they also knew that Dr. Zhu kept the laptop in his possession, rather than leaving it in his office, and that he alone used and had access to it is unclear on the current evidentiary record and should be determined at an evidentiary hearing.

At a minimum, the agents had an obligation to inquire into those matters before concluding that NYU had authority to consent to search of the laptop's contents. *See id*. at *15. As the Sixth Circuit has observed, "[t]he government cannot establish that its agents reasonably relied upon a third party's apparent authority if agents, faced with an ambiguous situation, nevertheless proceed without making further inquiry." *United States v. Waller*, 426 F.3d 838, 846 (6th Cir. 2005) (quotation omitted); *see, e.g., United States v. Purcell*, 526 F.3d 953, 963-64

(6th Cir. 2008) ("When a situation starts as unambiguous but subsequent discoveries create ambiguity, any apparent authority evaporates."); *United States v. Durham*, 1998 U.S. Dist. LEXIS 15482, at *11-*12 (D. Kan. Sept. 11, 1998) ("[The court is convinced, from the evidence produced at the hearing, that Special Agent Quinn, when it became apparent that the room was locked and that Mrs. Durham had no keys, unjustifiably failed to make reasonable inquiry into her authority to consent."). Here, the searching agents--at a minimum--had a duty to inquire further when they became aware that the laptop was password protected and encrypted and that NYU did not possess the passwords and could not undo the encryption.

Because the government lacked a warrant authorizing the search of the laptop, and because it cannot establish that the consent exception to the warrant requirement applies, the search violated Dr. Zhu's Fourth Amendment rights. *See, e.g., Griswold*, 2011 U.S. Dist. LEXIS 153943, at *39-*42.

III. THE CONTENTS OF THE LAPTOP, AND THE FRUITS OF THOSE CONTENTS, MUST BE SUPPRESSED.

The warrantless search of the laptop computer without proper consent violated Dr. Zhu's Fourth Amendment right to be protected from unreasonable searches and seizures. Accordingly, the evidence obtained from the search, and the fruits of that evidence, must be suppressed. *See Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963).

CONCLUSION

For the foregoing reasons, the Court should enter an Order suppressing all evidence obtained from the search of the laptop computer that Dr. Zhu surrendered to NYU in May 2013, and the fruits of that evidence. To the extent there are factual disputes material to a determination of the motion, the Court should conduct an evidentiary hearing.

Dated: March 14, 2014

Respectfully submitted,
/s/ John D. Cline

JOHN D. CLINE
Law Office of John D. Cline
235 Montgomery Street, Suite 1070
San Francisco, CA 94104
415.322.8319 (telephone)
415.524.8265 (facsimile)
Email: cline@johndclinelaw.com

/s/ Maurice Sercarz

MAURICE SERCARZ
Sercarz & Riopelle, LLP
810 Seventh Ave., Suite 620
New York, NY 10019
212.586.4900 (telephone)
212.586.1234 (facsimile)
Email: msercarz@sercarzandriopelle.com

CERTIFICATE OF SERVICE

This is to certify that on this the 14th day of March, 2014, I caused to be filed a true and correct copy of the instant Memorandum and annexed declarations using the Southern District of New York's Electronic Case Filing system ("ECF") which will send a notice of filing to all counsel of record.

/s/ John D. Cline
JOHN D. CLINE